Application Note 18

TransPort Security Lockdown

Digi Technical Support

February 2018

Contents

1 Introduction 5
1.1 Outline 5
1.2 Assumptions 5
1.3 Corrections 5
1.4 Version 5
2 Features to Consider when Securing a TransPort 6
2.1 Security Checklist 6
3 Introduction on Using This Guide 6
3.1 How to Use This Guide 6
4 Using Digi Remote Manager to Access TransPorts 7
4.1 Digi Remote Manager 7
5 Changing Default Username and Password & Using Password Encryption 7
5.1 Changing the Default Username and Password 7
5.1.1 WebUI Method 8
5.1.2 CLI Method 9
5.1.3 Digi Remote Manager Method 9
5.2 Using Encrypted Passwords 10
5.2.1 WebUI Method 10
5.2.2 CLI Method 11
5.2.3 Digi Remote Manager Method 11
6 Serial Port Security 12
6.1 Securing the Serial Ports 12
6.1.1 WebUI Method 12
6.1.2 CLI Method 13
6.1.3 Digi Remote Manager Method 13
7 Secure the USB Port 14
7.1 Functions of the USB Port 14

7.1.1 WebUI Method 14
7.1.2 CLI Method 15
7.1.3 Digi Remote Manager Method 15
8 Securing Ethernet Ports 17
8.1 Overview 17
8.1.1 WebUI Method 17
8.1.2 CLI Method 18
8.1.3 Digi Remote Manager Method 18
9 Enable the Firewall 19
9.1 Overview 19
9.1.1 WebUI Method 19
9.1.2 CLI Method 20
9.1.3 Digi Remote Manager Method 20
10 Disabling Insecure/Unneeded Management Protocols 21
10.1 Overview 21
10.2 Enable and Use HTTPS over HTTP 21
10.2.1 WebUI Method 21
10.2.2 CLI Method 22
10.2.3 Digi Remote Manager Method 22
10.3 Use SSH over Telnet 22
10.3.1 WebUI Method 22
10.3.2 CLI Method 23
10.3.3 Digi Remote Manager Method 23
10.4 Use SFTP over FTP 24
10.4.1 WebUI Method 24
10.4.2 CLI Method 24
10.4.3 Digi Remote Manger Method 24
10.5 Disable Serial TCP Ports 25
10.5.1 WebUI Method 25

10.5.2 CLI Method ... 25
10.5.3 Digi Remote Manager Method ... 25
10.6 Disable ADDP & ZING ... 26
10.6.1 WebUI Method ... 26
10.6.2 CLI Method ... 27
10.6.3 Digi Remote Manager Method ... 27
11 RADIUS & TACACS+ AAA Security ... 27
11.1 Why use RADIUS or TACACS+ ... 27
11.2 Enabling RADIUS ... 27
11.2.1 WebUI Method ... 28
11.2.2 CLI Method ... 28
11.2.3 Digi Remote Manager Method ... 29
11.3 Enabling TACACS+ ... 29
11.3.1 WebUI Method ... 29
11.3.2 CLI Method ... 30
11.3.3 Digi Remote Manager Method ... 31
12 Physical Security ... 32
12.1 Why Physical Security Important ... 32
12.2 Security Recommendations ... 32

1 INTRODUCTION

1.1 Outline

The purpose of this document is to cover a list of items to consider when securing the TransPort family of routers. The topics will include username & password changes, firewall suggestions, and using secure services to name a few.

1.2 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product and of the requirements for their specific application. It also assumes a basic ability to access and navigate a Digi TransPort router and configure it with basic routing functions.

This application note applies to:

Model: Digi TransPort WR21

Other Compatible Models: Digi TransPort WR family

Firmware versions: This document applies to firmware version 5.2.19.11 and later

Configuration: This Application Note assumes the devices are set to their factory default configurations. Most configuration commands are only shown if they differ from the factory default.

1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: tech.support@digi.com

Requests for new application notes can be sent to the same address.

1.4 Version

Version Number	Status
0.1	Draft
1.0	Initial Release

2 FEATURES TO CONSIDER WHEN SECURING A TRANSPORT

2.1 Security Checklist

The following list of items should be considered when starting the process of locking down a Digi TransPort cellular router:

- Using Digi Remote Manager to access devices
- Change the default username and password & use password encryption
- Secure unused serial port(s)
- Secure the USB port
- Secure unused Ethernet port(s)
- Enable Firewall
- Disabling insecure or unneeded management protocols
    a. Enable and use HTTPS with certificates, not HTTP
    b. Use SSH, not telnet
    c. Use SFTP or SCP, not FTP
    d. Disable Serial TCP ports
    e. Disable ADDP & Zing
- RADIUS & TACACS+ AAA Security
- Physical device security

This list can be used as a checklist when securing the router.

The next sections of this guide will cover each of these topics. If more detailed information of these topics is desired, please refer to the **Digi TransPort User Guide**, or by visiting the Digi Support website at http://www.digi.com/support.

3 INTRODUCTION ON USING THIS GUIDE

3.1 How to Use This Guide

This guide will cover 3 methods for configuring each of the topics that are covered. The 3 methods shown will be:

1. Using the Web User Interface (WebUI)
2. Using the Command Line Interface (CLI)
3. Using Digi Remote Manager (DRM)

Please take note of the particular method discussed when reviewing the topics of this guide, to ensure the correct steps are followed for the desired access method.

4 USING DIGI REMOTE MANAGER TO ACCESS TRANSPORTS

4.1 Digi Remote Manager

The Digi Remote Manager (DRM) platform is cloud-based system that allows for remote monitoring and control of all TransPort routers from a central location. It also has capabilities of keeping devices in compliance with a set policy on firmware, configuration files, and files on the file system.

DRM allows for the same capabilities of controlling the TransPorts that if found within the local WebUI. The same level of control is contained within the cloud platform.

DRM even allows for CLI access to the TransPort routers using the built-in “Execute a command” function, found under the Properties section of each router. This allows for most CLI commands that could be executed locally on a TransPort router to be issued from DRM through the cloud connection. The DRM CLI access is not fully interactive as a local CLI session would be, as such using certain commands may not provide the desired output. (e.g. – Running Python scripts will not provide feedback from print statements as would be seen over a local CLI session, but can be started from the DRM CLI session.)

DRM also has Profile Management options to allow the platform to perform period checks against the attached TransPorts, looking for items such as firmware versions being out of sync, the configuration of the devices being misaligned, and if the files on the local file system are the files that are expected to be there. DRM can then take action against these items of interest, and bring them into compliance with a pre-set group of values and/or firmware/file versions.

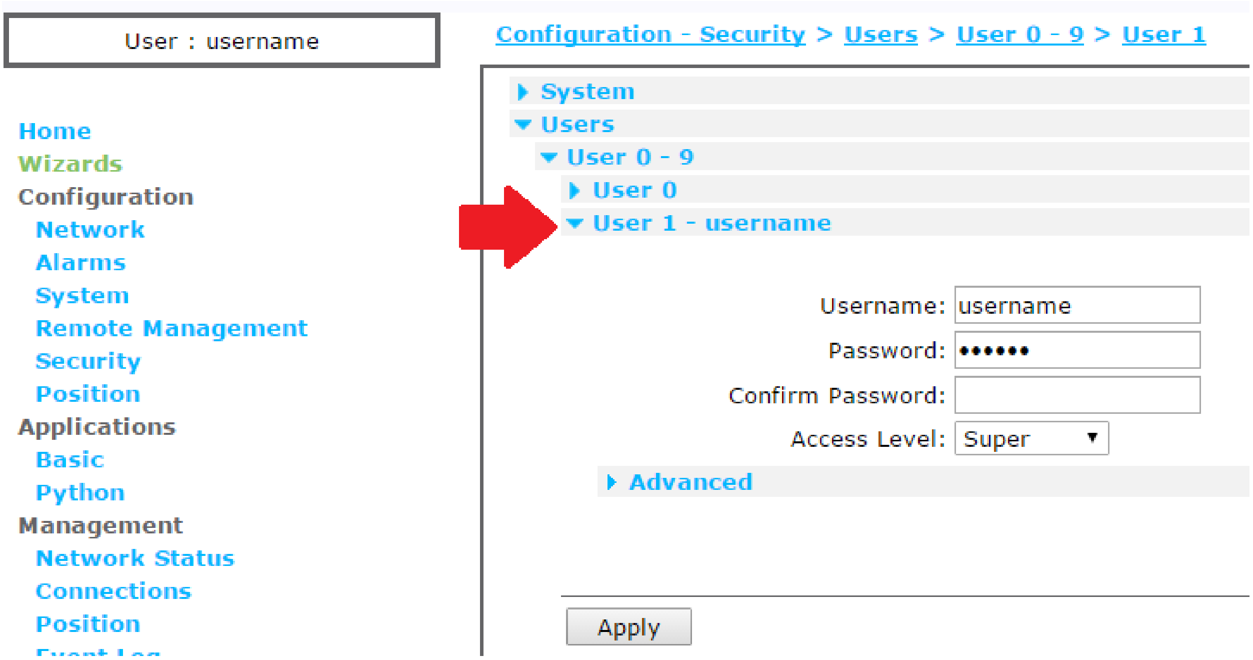
5 CHANGING DEFAULT USERNAME AND PASSWORD & USING PASSWORD ENCRYPTION

5.1 Changing the Default Username and Password

Like most routers, the Digi TransPort comes with a default username and password, which are ‘username’ and ‘password’ respectively. These are well known to anyone that can view Digi documentation that lists this information, so it is highly recommended as the first step in securing the router to change these defaults to something more secure.

5.1.1 WebUI Method

Log into the WebUI with the existing username and password, navigate to **Configuration – Security > Users > User 0 - 9 > User 1**, as shown below:



Username: username

Password: ••••••

Confirm Password:

Access Level: Super

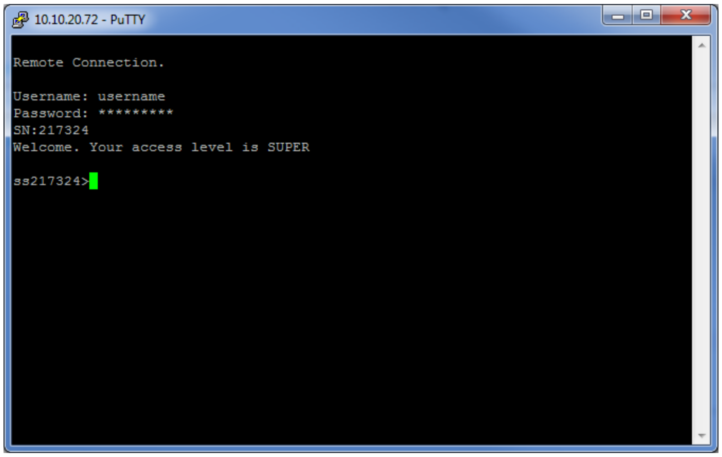
Change the username and password to something more secure than the defaults. If "Super" user access is not necessary, this can also be lowered. More information on the user levels that are supported on the TransPort can be found in the "**User Security Settings**" section in the Digi TransPort Users Guide on the Digi Support website.

NOTE: If "Super" user access is removed and no other user is setup for Super user access, a factory default of the TransPort may be required to reset the user back to default access. Digi Remote Manager is also another way around this issue, as the user access can be reset via DRM.

After the username and password have been changed, click **Apply** and **Save** the configuration changes for them to take effect immediately.

5.1.2 CLI Method

Using Telnet or SSH, log into the CLI of the TransPort to see a prompt similar to the below screenshot:



```
Remote Connection.

Username: username
Password: *********
SN:217324
Welcome. Your access level is SUPER

ss217324>
```

Once at the CLI, use the following commands to change the username and password:

user 1 name new_username
user 1 password new_password
config 0 save

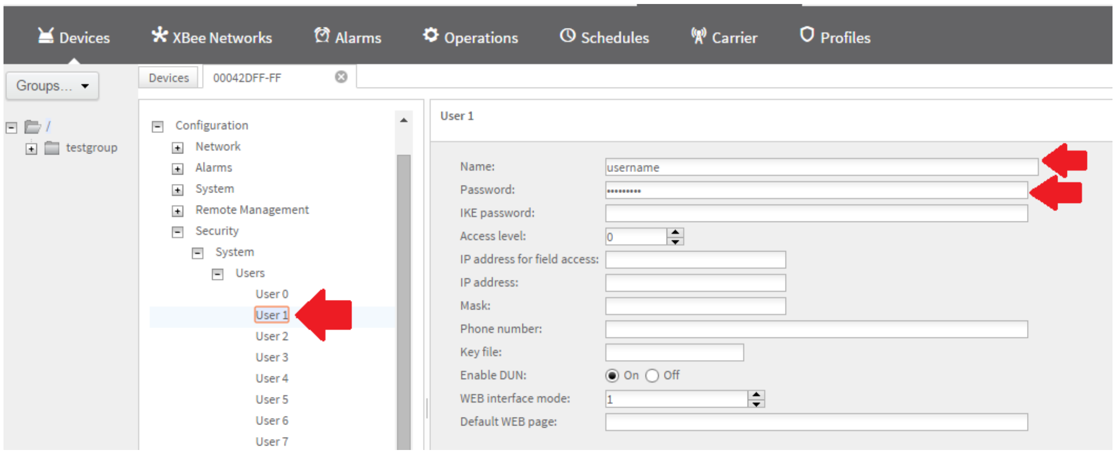
This will change the username and password to the new settings immediately.

NOTE: Although the password will be entered in as plaintext, the password will automatically become enciphered or encrypted after it is entered into the TransPort.

5.1.3 Digi Remote Manager Method

Inside of Digi Remote Manager, navigate to **Device Management > Devices**, and open up the **Properties** of the device to change.

Once on the Properties page, navigate to **Configuration > Security > System > Users > User 1**, and change the “Name” and “Password” fields, as shown below:



User 1

Name:	username
Password:	•••••••••
IKE password:	
Access level:	0
IP address for field access:	
IP address:	
Mask:	
Phone number:	
Key file:	
Enable DUN:	● On ○ Off
WEB interface mode:	1
Default WEB page:	

Click the **Save** button at the bottom of the page to commit the changes to the TransPort immediately.

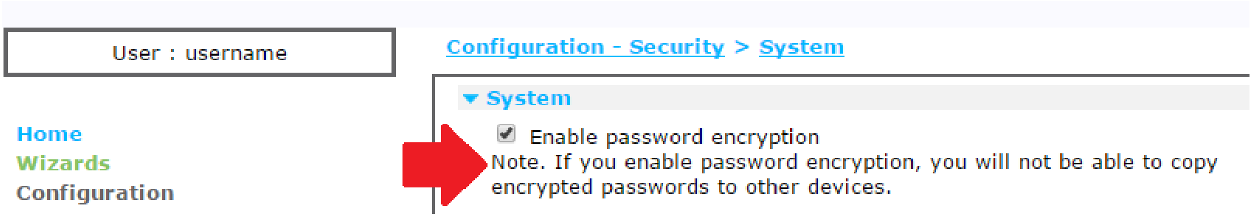
5.2 Using Encrypted Passwords

The TransPort by default does not use password Encryption, but rather has Obfuscated passwords enabled. Starting with firmware 5.2.9.13 and later, the TransPort now offers the ability to encrypt the passwords instead of just obfuscating the passwords.

NOTE: Encrypted passwords are specific to the device they were created on, and cannot be copied to any other devices to be read. What this means is if a device is to be used as a template for other devices of a similar model, **do not** backup the configuration while the device is in Encrypted mode, otherwise the backup file cannot be loaded onto any other devices to read the passwords in the file, thus making the backup file useless except for the one device it was created from.

5.2.1 WebUI Method

Navigate to **Configuration – Security > System**, and check the box for **Enable password encryption** to encrypt the current passwords, as shown below:



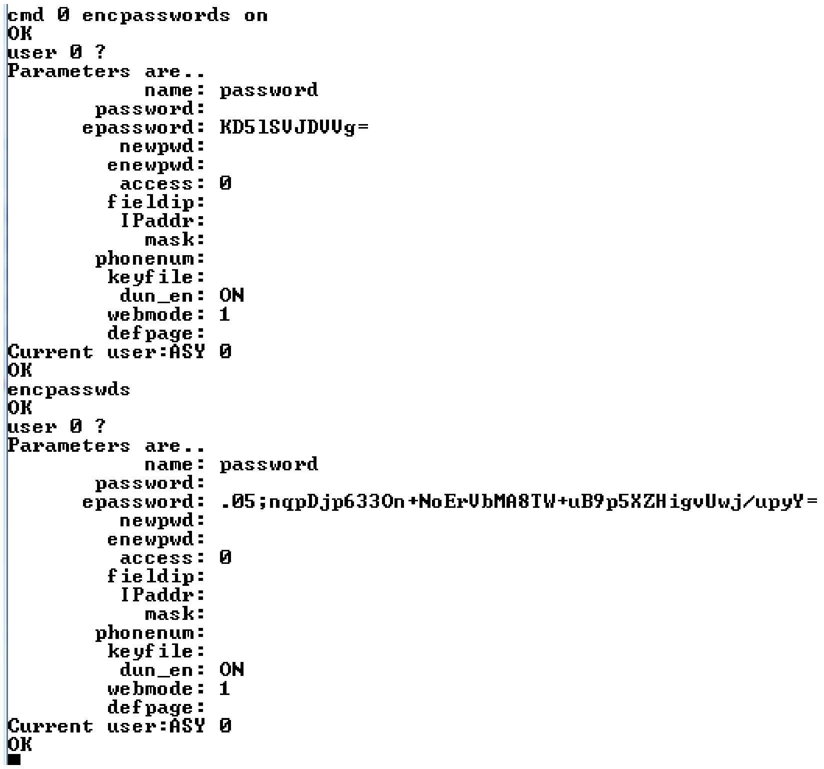
☑ Enable password encryption

Note. If you enable password encryption, you will not be able to copy encrypted passwords to other devices.

Make sure to **Apply** and **Save** the changes after enabling the option.

NOTE: This alone will not encrypt the passwords on the device. The passwords will need to be re-entered manually to become encrypted, or run the command '**encpasswds**' from the CLI to encrypt all existing passwords at once.

The screenshot on the next page shows what a password looks like before and after encryption has been applied with the 'encpasswds' command (see the "epassword" field below):



```
cmd 0 encpasswords on
OK
user 0 ?
Parameters are..
           name: password
       password:
      epassword: KD51SVJDVVg=
         newpwd:
        enewpwd:
         access: 0
        fieldip:
         IPaddr:
           mask:
       phonenum:
        keyfile:
         dun_en: ON
        webmode: 1
        defpage:
Current user:ASY 0
OK
encpasswds
OK
user 0 ?
Parameters are..
           name: password
       password:
      epassword: .05;nqpDjp633On+NoErVbMA8TW+uB9p5XZHigvUwj/upyY=
         newpwd:
        enewpwd:
         access: 0
        fieldip:
         IPaddr:
           mask:
       phonenum:
        keyfile:
         dun_en: ON
        webmode: 1
        defpage:
Current user:ASY 0
OK
```

5.2.2 CLI Method

To encrypt the passwords from the CLI, log into the TransPort using Telnet or SSH, and issue the following commands:

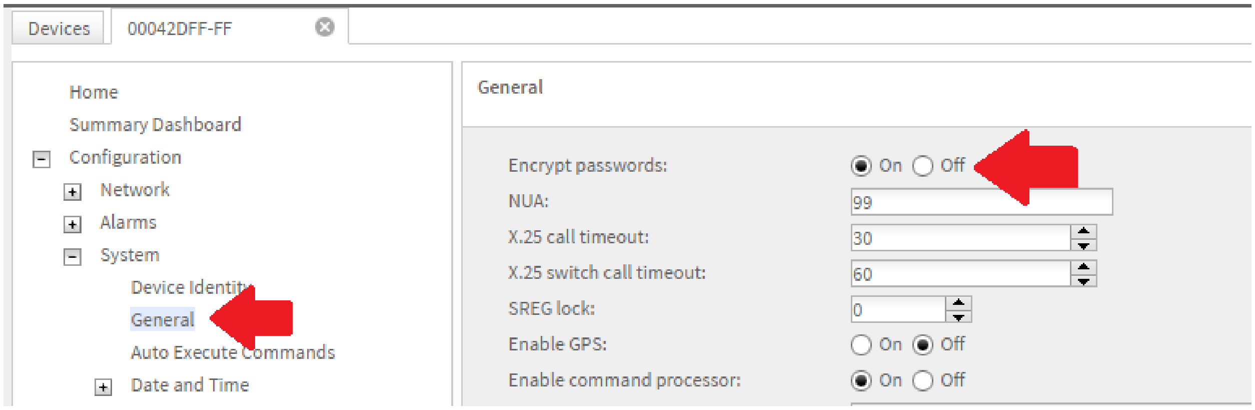
cmd 0 encpasswords on
config 0 save

NOTE: This alone will not encrypt the passwords on the device. The passwords will need to be re-entered manually to become encrypted, or run the command '**encpasswds**' from the CLI to encrypt all passwords at once.

5.2.3 Digi Remote Manager Method

Inside of Digi Remote Manager, navigate to **Device Management > Devices**, and open up the **Properties** of the device to change.

Once on the Properties page, navigate to **Configuration > System > General**, and change the "Encrypt passwords" field to "On", as shown on the next screenshot:



General

Encrypt passwords: ● On ○ Off
NUA: 99
X.25 call timeout: 30
X.25 switch call timeout: 60
SREG lock: 0
Enable GPS: ○ On ● Off
Enable command processor: ● On ○ Off

Click the **Save** button at the bottom of the page to commit the changes to the TransPort immediately.

NOTE: This alone will not encrypt the passwords on the device. The passwords will need to be re-entered manually to become encrypted, or run the command '**encpasswds**' from the **Administration > Execute a command** section in DRM to encrypt all passwords at once.

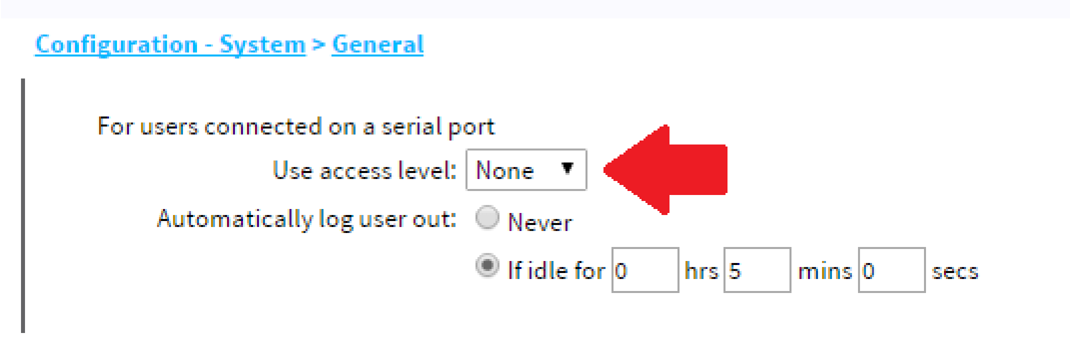
6 SERIAL PORT SECURITY

6.1 Securing the Serial Ports

By default, the serial ports on the TransPort routers do not have security enabled. The serial ports will provide direct access to the CLI of the TransPort with Super user privileges, and allow for any command to be issue by that user. If the serial ports are not in use by some other device/application, it is recommended to add security to the ports to prevent unwanted access.

6.1.1 WebUI Method

Navigate to **Configuration – System > General**, and change the **Use access level** drop down from "Super" to the appropriate user level, as shown below:



For users connected on a serial port
Use access level: None
Automatically log user out: ○ Never
● If idle for 0 hrs 5 mins 0 secs

NOTE: With the access level of '**None**' chosen, the command '**login**' can still be issued on the serial port to be able to log into the system with the appropriate system user, and the '**logout**' command is used to close the session when finished.

It is also recommended to set an idle timeout for the users logging into the CLI via the serial port. This helps prevent users staying logged permanently in to the serial port if they forget to logout when finished (which is the default behavior).

Make sure to **Apply** and **Save** the changes after they are made in the WebUI to take effect.

6.1.2 CLI Method

To enable logins on the serial port from the CLI, log into the TransPort using Telnet or SSH, and issue the following commands:

local 0 access x (where 'x' equals: 0=Super, 1=High, 2=Med, 3=Low, 4=None)
local 0 tlocto x (where 'x' equals time in seconds for the idle timeout)
config 0 save

These commands will set the user level of the serial port, and also enable an idle timeout on the port.

6.1.3 Digi Remote Manager Method

The Digi Remote Manager option for securing the serial port(s) is the same as the CLI commands used in the previous section. Within Digi Remote Manager, navigate to **Device Management > Devices**, and open up the **Properties** of the device to change.

Once on the Properties page, navigate to **Administration > Execute a command**. On this page, enter in the following commands:

local 0 access x (where 'x' equals: 0=Super, 1=High, 2=Med, 3=Low, 4=None)
local 0 tlocto x (where 'x' equals time in seconds for the idle timeout)
config 0 save

7 SECURE THE USB PORT

7.1 Functions of the USB Port

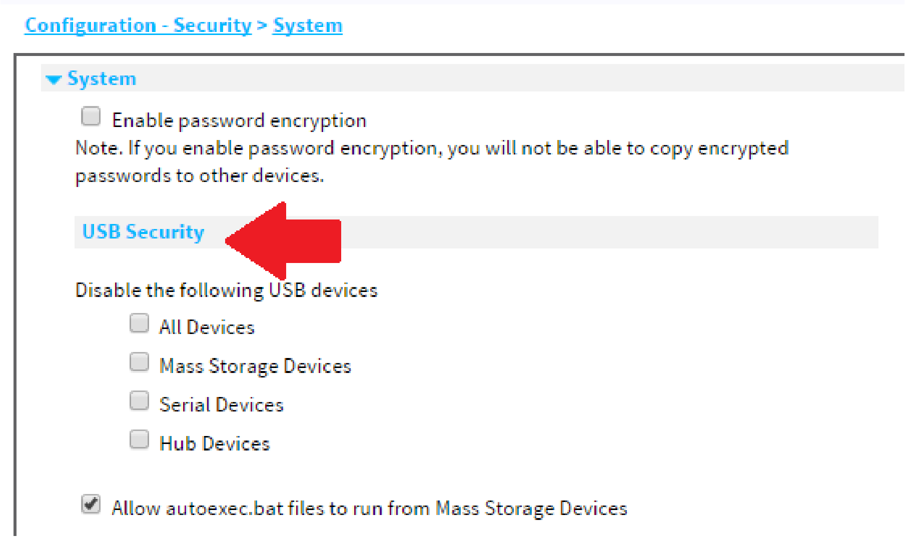
The USB port on the TransPort router works with a few types of devices, which include:

- USB Mass Storage Devices (Flash Drives)
- Extra Serial Ports & GPS Receiver (FTDI and Prolific chipsets only)
- USB Hubs

By default, the TransPort will allow any of these types of devices to be connected and used through the device without restrictions. This section will go over the options of disabling these features if they are not being used.

7.1.1 WebUI Method

Navigate to **Configuration – Security > System**, and locate the section title **USB Security**, as shown on the next page:



Configuration - Security > System

System

□ Enable password encryption

Note. If you enable password encryption, you will not be able to copy encrypted passwords to other devices.

USB Security

Disable the following USB devices

□ All Devices

□ Mass Storage Devices

□ Serial Devices

□ Hub Devices

☑ Allow autoexec.bat files to run from Mass Storage Devices

Under this section, there is the ability to turn off the use of all USB devices on the port, or the 3 individual items previously mentioned. If the USB port will not be used, the selection 'All Devices' can be used to disable the use of any USB devices on the TransPort.

If Mass Storage Devices are still allowed to be used on the TransPort, the option for "Allow autoexec.bat files to run from Mass Storage Devices" should be considered when locking the router down. This option allows for 'autoexec.bat' files to execute on the Mass Storage Device when they are plugged into the router. Disable this feature if the Mass Storage Devices are not used to automatically run files on the TransPort.

Make sure to **Apply** and **Save** the changes to take effect.

7.1.2 CLI Method

To disable options of the USB port from the CLI, log into the TransPort using Telnet or SSH, and issue the following commands:

Disable All Devices:
usbcon 0 dislist "usb-err-err.*“

Disable Mass Storage Devices:
usbcon 0 dislist "usb-err-err.MSD“

Disable Serial Devices:
usbcon 0 dislist "usb-err-err.SERIAL“

Disable USB Hubs:
usbcon 0 dislist "usb-err-err.HUB"

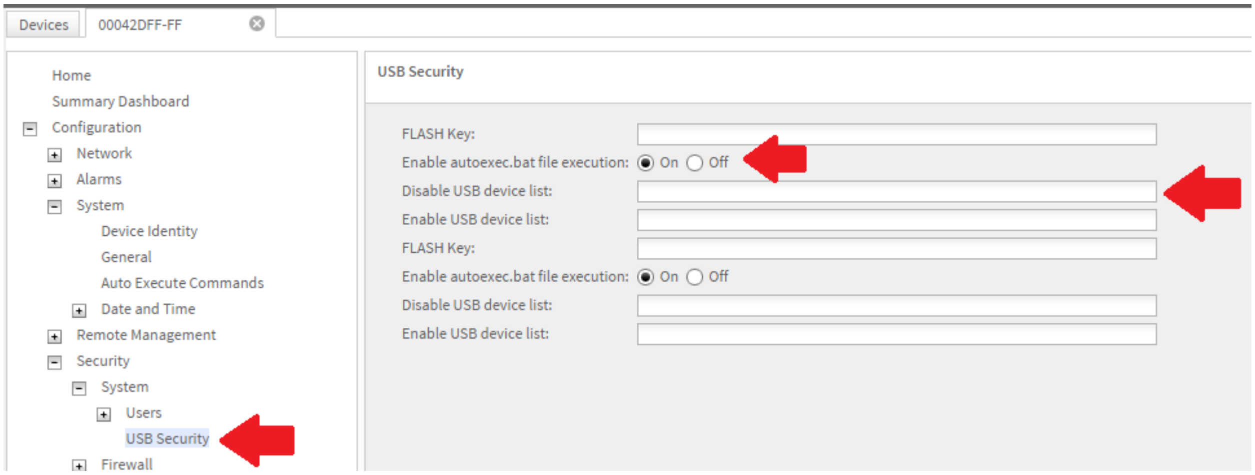
Disable autoexec batch file:
usbcon 0 batfile OFF

Ensure to run the command ‘**config 0 save**’ after executing any of the above commands to save the changes.

7.1.3 Digi Remote Manager Method

Inside of Digi Remote Manager, navigate to **Device Management > Devices**, and open up the **Properties** of the device to change.

Once on the Properties page, navigate to **Configuration > Security > System > USB Security**. On this page, there are 2 fields of importance: 1) Enable autoexec.bat file execution, and 2) Disable USB device list, both of which are highlighted in the screenshot below:



USB Security

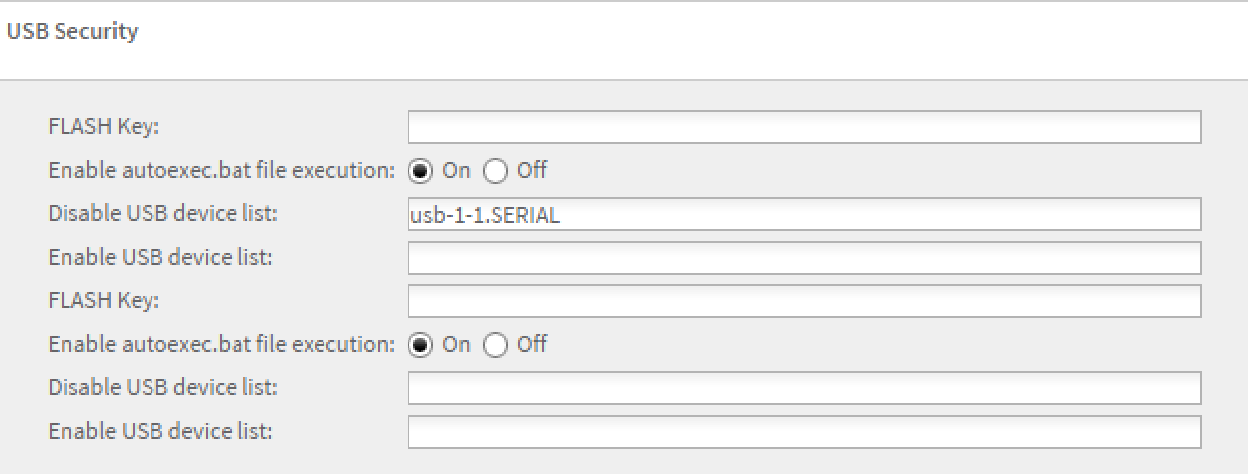
FLASH Key:
Enable autoexec.bat file execution: ● On ○ Off
Disable USB device list:
Enable USB device list:
FLASH Key:
Enable autoexec.bat file execution: ● On ○ Off
Disable USB device list:
Enable USB device list:

The first field, **Enable autoexec.bat file execution**, enables/disables the use of ‘autoexec.bat’ files from Mass Storage Devices.

The second field, **Disable USB device list**, is where the various USB device are listed that should be disabled. The options for this field are:

usb-1-1.* <- This option disables all USB devices on the port.
usb-1-1.MSD <- This option disables Mass Storage Devices only.
usb-1-1.SERIAL <- This option disables Serial Devices only.
usb-1-1.HUB <- This option disables Hub Devices only.

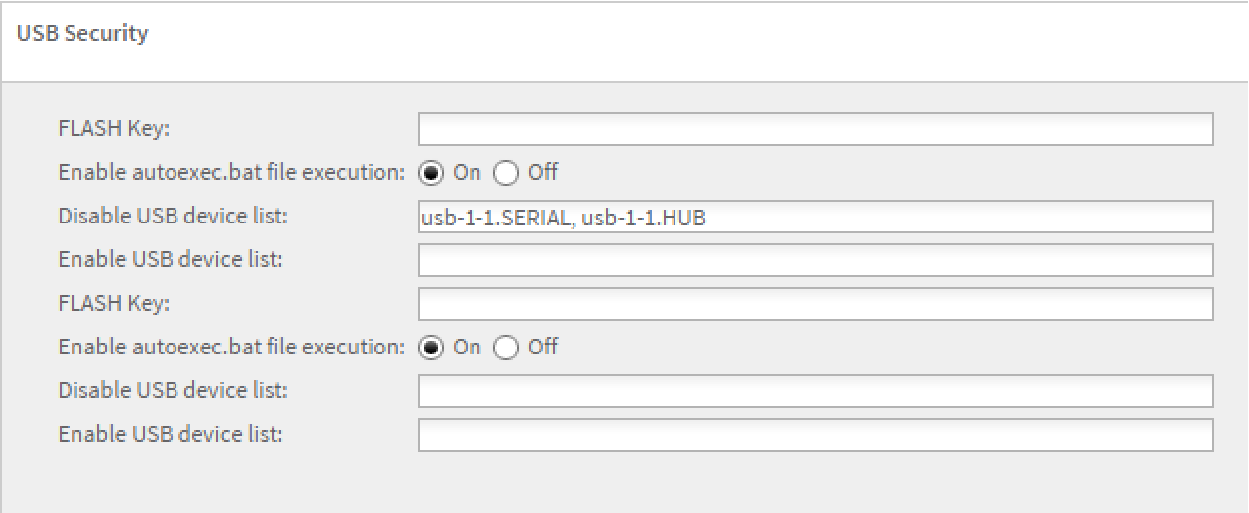
For example, if only Serial Devices were to be disabled, the setup would look like this:



USB Security

FLASH Key:	
Enable autoexec.bat file execution:	● On ○ Off
Disable USB device list:	usb-1-1.SERIAL
Enable USB device list:	
FLASH Key:	
Enable autoexec.bat file execution:	● On ○ Off
Disable USB device list:	
Enable USB device list:	

More than 1 option can also be listed on the same line, with the options being separated by a comma. For example, if both Serial Devices and Hub Devices needed to be disabled, the setup would look like this:



USB Security

FLASH Key:	
Enable autoexec.bat file execution:	● On ○ Off
Disable USB device list:	usb-1-1.SERIAL, usb-1-1.HUB
Enable USB device list:	
FLASH Key:	
Enable autoexec.bat file execution:	● On ○ Off
Disable USB device list:	
Enable USB device list:	

Once finished, click the **Save** button at the bottom of the page to commit the changes to the TransPort immediately.

8 SECURING ETHERNET PORTS

8.1 Overview

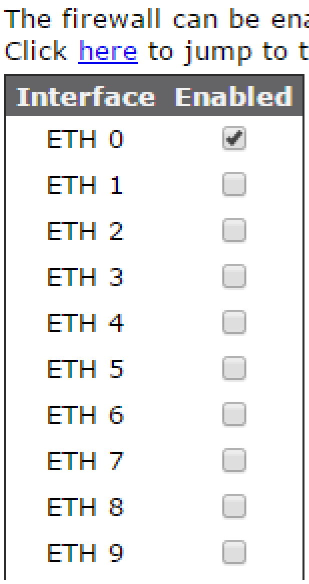
All TransPort routers with multiple Ethernet ports, by default, come in ‘hub mode’, where all of the Ethernet ports are linked together as a hub, and function just like a hub. If these items are not taken into consideration, there is potential that unwanted access to the TransPort can occur:

- Enable the firewall on the Ethernet ports to allow/deny traffic
- Disable management access over the Ethernet ports

8.1.1 WebUI Method

8.1.1.1 Enabling the Firewall

Navigate to **Configuration – Security > Firewall**. Once there, check the box for ETH x (where ‘x’ is the interface number) to enable the firewall on a given interface, as shown below:



The firewall can be enabled on Ethernet, PPP and GRE interfaces.
Click here to jump to the GRE configuration page.

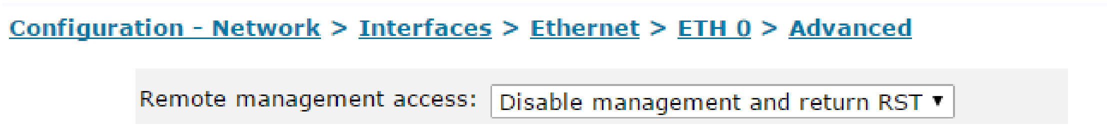
Interface	Enabled
ETH 0	☑
ETH 1	☐
ETH 2	☐
ETH 3	☐
ETH 4	☐
ETH 5	☐
ETH 6	☐
ETH 7	☐
ETH 8	☐
ETH 9	☐

Click **Apply** and **Save** the changes after this option has been set.

NOTE: If the firewall rules are not edited properly, it is possible to lock out all access from the TransPort router once the firewall is enabled. If this happens, a factory default may be necessary to gain access back into the router if no holes were left open within the firewall.

8.1.1.2 Disabling Management on Ethernet Ports

Navigate to **Configuration – Network > Interfaces > Ethernet > ETH x > Advanced**. Locate the setting for **Remote management access**, and change this parameter to **Disable management and return RST**, as shown on the next page:



Configuration - Network > Interfaces > Ethernet > ETH 0 > Advanced

Remote management access: Disable management and return RST ▾

Click **Apply** and **Save** the changes after this option has been set.

Once this is saved, it is no longer possible to gain access to management ports on the TransPort over this interface.

8.1.2 CLI Method

8.1.2.1 Enabling the Firewall

To enable the firewall using the CLI, log into the TransPort using Telnet or SSH, and issue the following commands:

eth x firewall on (where 'x' equals the Ethernet interface number)
config 0 save

8.1.2.2 Disabling Management on Ethernet Ports

To disable management on Ethernet interfaces using the CLI, log into the TransPort using Telnet or SSH, and issue the following commands:

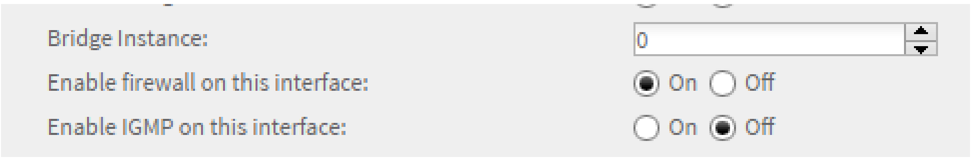
eth x nocfg to 3 (where 'x' equals the Ethernet interface number)
config 0 save

8.1.3 Digi Remote Manager Method

8.1.3.1 Enabling the Firewall

Inside of Digi Remote Manager, navigate to **Device Management > Devices**, and open up the **Properties** of the device to change.

Once on the Properties page, navigate to **Configuration > Network > Interfaces > Ethernet > Ethernet x**. On this page, look for the field titled **Enable firewall on this interface**, and change this to *On*, as shown below:



Bridge Instance: 0

Enable firewall on this interface: ● On ○ Off

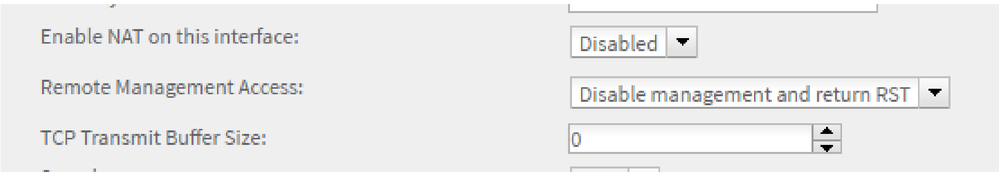
Enable IGMP on this interface: ○ On ● Off

Ensure to **Save** the change after it is made.

8.1.3.2 Disabling Management on Ethernet Ports

Inside of Digi Remote Manager, navigate to **Device Management > Devices**, and open up the **Properties** of the device to change.

Once on the Properties page, navigate to **Configuration > Network > Interfaces > Ethernet > Ethernet x**. On this page, look for the field titled **Remote Management Access**, and change this to *Disable management and return RST*, as shown below:



Enable NAT on this interface: Disabled

Remote Management Access: Disable management and return RST

TCP Transmit Buffer Size: 0

Ensure to **Save** the change after it is made.

9 ENABLE THE FIREWALL

9.1 Overview

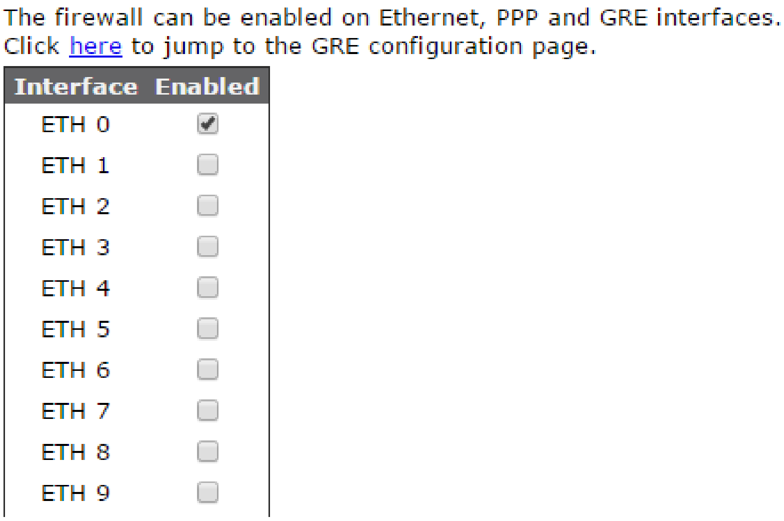
The TransPort family of routers has an Enterprise class firewall built-in to the devices that can be enabled to protect the router from unwanted traffic and access. The default rules that come with the TransPort only allow for the following:

1) Allow all traffic to leave the router and allow replies back in for that traffic.
2) Allow IPSec traffic to pass.
3) Allow incoming SSH and HTTPS for management.
4) Block all other traffic

With the default rules enabled, the router is relatively locked down from an outside, open port perspective. These rules can be edited to allow for whichever type of traffic is needed to pass through the router. **This section will not go over specific firewall rules, but how to enable the firewall on the various interfaces.**

9.1.1 WebUI Method

Navigate to **Configuration – Security > Firewall**. Once there, check the box for the interface to enable the firewall on a given interface (i.e. – ETH 0, ETH 1, PPP 1, PPP 2, etc.), as shown below:



The firewall can be enabled on Ethernet, PPP and GRE interfaces.
Click here to jump to the GRE configuration page.

Interface	Enabled
ETH 0	☑
ETH 1	□
ETH 2	□
ETH 3	□
ETH 4	□
ETH 5	□
ETH 6	□
ETH 7	□
ETH 8	□
ETH 9	□

Click **Apply** and **Save** the changes after this option has been set.

NOTE: If the firewall rules are not edited properly, it is possible to lock out all access from the TransPort router once the firewall is enabled. If this happens, a factory default may be necessary to gain access back into the router if no holes were left open within the firewall.

9.1.2 CLI Method

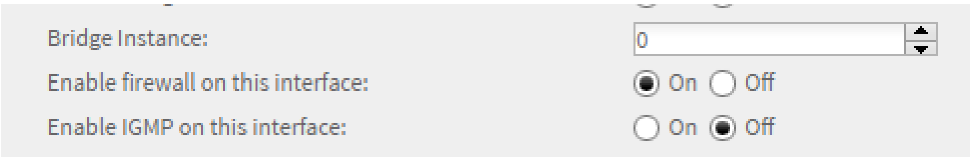
To enable the firewall using the CLI, log into the TransPort using Telnet or SSH, and issue the following commands:

ppp x firewall on (where ‘x’ equals the PPP interface number; typically 1)
eth x firewall on (where ‘x’ equals the Ethernet interface number)
config 0 save

9.1.3 Digi Remote Manager Method

Inside of Digi Remote Manager, navigate to **Device Management > Devices**, and open up the **Properties** of the device to change.

Once on the Properties page, navigate to **Configuration > Network > Interfaces > Ethernet > Ethernet x** for *Ethernet interfaces*, or navigate to **Configuration > Network > Interfaces > Advanced > PPP x** for *Mobile interfaces*. On this page, look for the field titled **Enable firewall on this interface**, and change this to *On*, as shown below:



Bridge Instance: 0
Enable firewall on this interface: ● On ○ Off
Enable IGMP on this interface: ○ On ● Off

Ensure to **Save** the change after it is made.

10 DISABLING INSECURE/UNNEEDED MANAGEMENT PROTOCOLS

10.1 Overview

For ease of use, there are several protocols that are enabled by default on the TransPort that are not as secure as an equal protocol on the device. This section will cover what those protocols are, and what can be done to make those types of connections more secure.

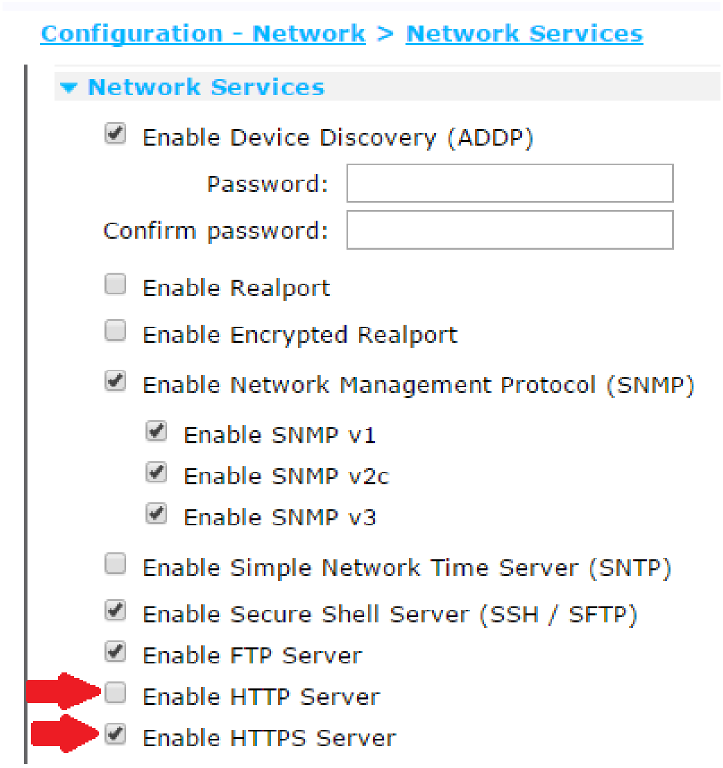
10.2 Enable and Use HTTPS over HTTP

The default web access method on the TransPort is the HTTP protocol. HTTP is not a secure protocol, as everything it sends/receives is in plain text. The alternative to using HTTP is to use the HTTPS protocol. This section will describe how to disable HTTP and enable HTTPS for a more secure connection.

NOTE: The default certificates that are used with HTTPS are certificates created by Digi International, and therefore are used on all TransPort routers by default. It is recommended that different certificates are created and used for the HTTPS connection to ensure a more secure connection.

10.2.1 WebUI Method

Navigate to **Configuration – Network > Network Services**, *uncheck* the box for **HTTP**, and *check* the box for **HTTPS**, as shown below:



Configuration - Network > Network Services

▾ Network Services

☑ Enable Device Discovery (ADDP)

Password:

Confirm password:

☐ Enable Realport

☐ Enable Encrypted Realport

☑ Enable Network Management Protocol (SNMP)

☑ Enable SNMP v1

☑ Enable SNMP v2c

☑ Enable SNMP v3

☐ Enable Simple Network Time Server (SNTP)

☑ Enable Secure Shell Server (SSH / SFTP)

☑ Enable FTP Server

☐ Enable HTTP Server

☑ Enable HTTPS Server

Apply and **Save** the changes after they are made.

NOTE: After **Apply** is selected at the bottom of the page, the HTTP connection that is currently being used to configure the TransPort will be lost due to the service now being disabled. In the web browser, a new connection will need to be made to the device using https://IP_of_TransPort to get back into the device to **Save** the changes.

10.2.2 CLI Method

To enable HTTPS and disable HTTP from the CLI, log into the TransPort using Telnet or SSH, and issue the following commands:

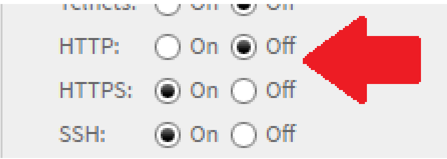
```
services 0 http off
services 0 https on
config 0 save
```

This will enable HTTPS and disable HTTP on the TransPort.

10.2.3 Digi Remote Manager Method

Within Digi Remote Manager, navigate to **Device Management > Devices**, and open up the **Properties** of the device to change.

Once on the Properties page, navigate to **Configuration > Network > Network Services**. On this page, set HTTP to **Off** and HTTPS to **On**, as shown below:



HTTP: ○ On ● Off

HTTPS: ● On ○ Off

SSH: ● On ○ Off

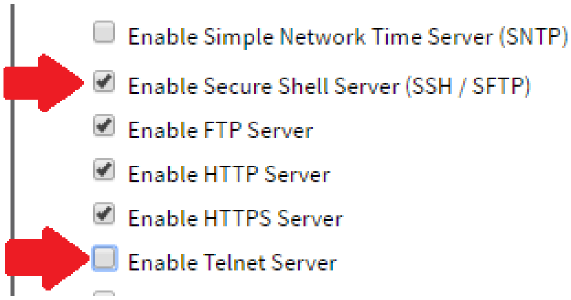
Ensure to **Save** the changes after they are made.

10.3 Use SSH over Telnet

The default CLI access methods on the TransPort both Telnet and SSH. Telnet is not a secure protocol, as everything it sends/receives is in plain text. It is recommended to disable Telnet if the service is not needed, as SSH can still be used for a secure command line connection. This section will describe how to disable Telnet.

10.3.1 WebUI Method

Navigate to **Configuration – Network > Network Services**, *uncheck* the box for **Enable Telnet Server**, and *check* the box for **Enable Secure Shell Server (SSH/SFTP)**, as shown below:



□ Enable Simple Network Time Server (SNTP)
☑ Enable Secure Shell Server (SSH / SFTP)
☑ Enable FTP Server
☑ Enable HTTP Server
☑ Enable HTTPS Server
□ Enable Telnet Server

Apply and **Save** the changes after they are made.

If a different port other than port 22 is desired for SSH connectivity, configure the SSH parameters under **Configuration – Network > SSH Server > SSH Server x**.

10.3.2 CLI Method

To enable SSH and disable Telnet from the CLI, log into the TransPort using SSH, and issue the following commands:

services 0 telnet off
services 0 ssh on
config 0 save

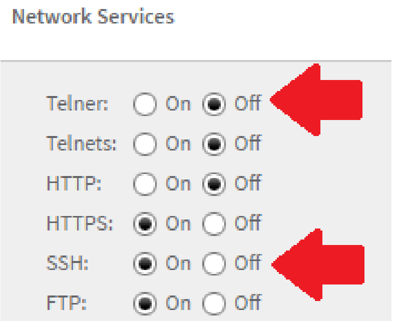
This will enable SSH and disable Telnet on the TransPort.

NOTE: The SSH Server has a separate configuration section for the server specific parameters. Use the command **ssh x ?** (where 'x' is the SSH instance number) to see the available parameters for the SSH server.

10.3.3 Digi Remote Manager Method

Within Digi Remote Manager, navigate to **Device Management > Devices**, and open up the **Properties** of the device to change.

Once on the Properties page, navigate to **Configuration > Network > Network Services**. On this page, set Telnet to **Off** and SSH to **On**, as shown below:



Network Services

Telner: ○ On ● Off
Telnets: ○ On ● Off
HTTP: ○ On ● Off
HTTPS: ● On ○ Off
SSH: ● On ○ Off
FTP: ● On ○ Off

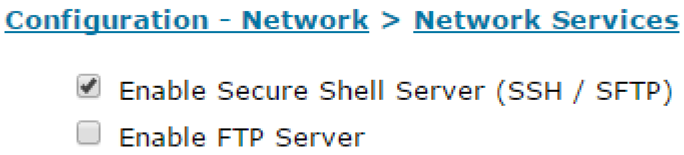
Ensure to **Save** the changes after they are made.

10.4 Use SFTP over FTP

Using SFTP over FTP will add a layer of security to the file transfers that can be made to/from the TransPort routers. This section will go through enabling this option on the TransPorts.

10.4.1 WebUI Method

First, navigate to **Configuration – Network > Network Services**, and ensure that **Enable Secure Shell Server (SSH/SFTP)** is enabled, and **Enable FTP Server** is disabled, as shown below:



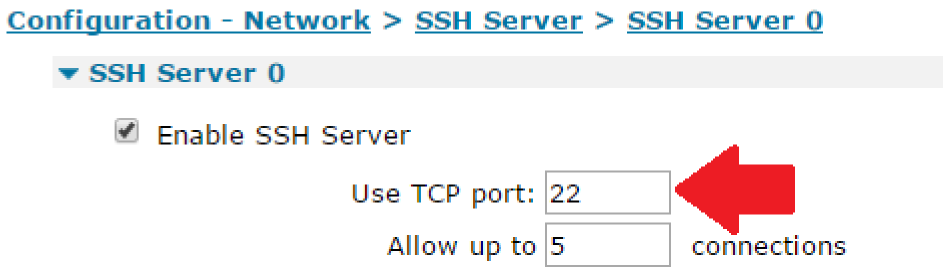
Configuration - Network > Network Services

☑ Enable Secure Shell Server (SSH / SFTP)

□ Enable FTP Server

Apply and **Save** this change.

After the change has been applied, the SFTP client should be able to reach the TransPort on standard port 22. This port can be changed under **Configuration – Network > SSH Server > SSH Server 0**, and changing the value for **Use TCP Port**, as shown below:



Configuration - Network > SSH Server > SSH Server 0

▼ SSH Server 0

☑ Enable SSH Server

Use TCP port: 22

Allow up to 5 connections

10.4.2 CLI Method

To enable SFTP and disable FTP from the CLI, log into the TransPort using SSH, and issue the following commands:

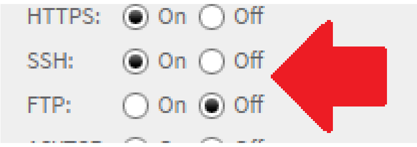
services 0 ftp off
services 0 ssh on <- This should be on by default.
ssh 0 port 22 <- This command is used to change the port number.
config 0 save

This will enable SFTP and disable FTP on the TransPort.

10.4.3 Digi Remote Manger Method

Within Digi Remote Manager, navigate to **Device Management > Devices**, and open up the **Properties** of the device to change.

Once on the Properties page, navigate to **Configuration > Network > Network Services**. On this page, set FTP to **Off** and SSH to **On**, as shown below:



HTTPS: ● On ○ Off
SSH: ● On ○ Off
FTP: ○ On ● Off

Ensure to **Save** the changes after they are made.

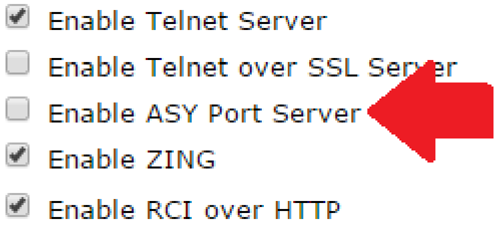
NOTE: If the port needs to be changed, this can be done under **Configuration > Network > SSH > SSH Server 0**.

10.5 Disable Serial TCP Ports

If the serial port(s) on the TransPort is/are unused, it is recommended to disable the TCP Server the ports have enabled by default. This section will go through disabling the TCP Server for these ports.

10.5.1 WebUI Method

Navigate to **Configuration – Network > Network Services**, and uncheck the option for **Enable ASY Port Server**, as shown below:



☑ Enable Telnet Server
□ Enable Telnet over SSL Server
□ Enable ASY Port Server
☑ Enable ZING
☑ Enable RCI over HTTP

Ensure to **Apply** and **Save** the changes after they are made.

10.5.2 CLI Method

To disable the serial port TCP Server from the CLI, log into the TransPort using SSH, and issue the following commands:

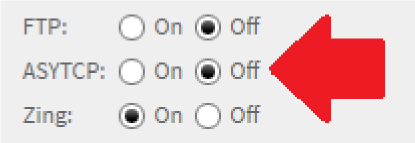
```
services 0 asytcp off
config 0 save
```

This will disable the TCP Server for the serial ports on the TransPort.

10.5.3 Digi Remote Manager Method

Within Digi Remote Manager, navigate to **Device Management > Devices**, and open up the **Properties** of the device to change.

Once on the Properties page, navigate to **Configuration > Network > Network Services**. On this page, set ASYTCP to **Off**, as shown below:



FTP: ○ On ● Off
ASYTCP: ○ On ● Off
Zing: ● On ○ Off

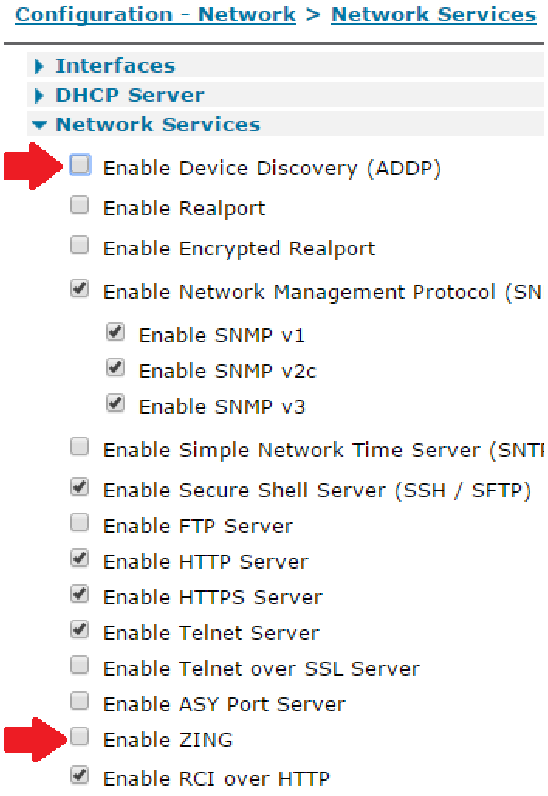
Ensure to **Save** the changes after they are made.

10.6 Disable ADDP & ZING

Both ADDP and ZING are protocols that are used for discovering the TransPort routers on a local network. These protocols will allow for the devices to be seen when running programs such as the Digi Device Discovery Tool, and will allow for items such as the IP address to be changed. These services should be disabled if they are unused.

10.6.1 WebUI Method

Navigate to **Configuration – Network > Network Services**, and uncheck the options for **Enable Device Discovery (ADDP)** and **Enable ZING**, as shown below:



Configuration - Network > Network Services

▸ Interfaces
▸ DHCP Server
▾ Network Services

☐ Enable Device Discovery (ADDP)
☐ Enable Realport
☐ Enable Encrypted Realport
☑ Enable Network Management Protocol (SN
☑ Enable SNMP v1
☑ Enable SNMP v2c
☑ Enable SNMP v3
☐ Enable Simple Network Time Server (SNT
☑ Enable Secure Shell Server (SSH / SFTP)
☐ Enable FTP Server
☑ Enable HTTP Server
☑ Enable HTTPS Server
☑ Enable Telnet Server
☐ Enable Telnet over SSL Server
☐ Enable ASY Port Server
☐ Enable ZING
☑ Enable RCI over HTTP

Ensure to **Apply** and **Save** the changes after they are made.

10.6.2 CLI Method

To disable ADDP and ZING from the CLI, log into the TransPort using SSH, and issue the following commands:

```
services 0 zing off
addp 0 enable off
config 0 save
```

This will disable both protocols on the TransPort.

10.6.3 Digi Remote Manager Method

The method for disabling ADDP and ZING from Digi Remote Manager are the same commands used for the CLI method above. Within Digi Remote Manager, navigate to **Device Management > Devices**, and open up the **Properties** of the device to change.

Once on the Properties page, navigate to **Administration > Execute a command**. On this page, run the following commands:

```
services 0 zing off
addp 0 enable off
config 0 save
```

11 RADIUS & TACACS+ AAA SECURITY

11.1 Why use RADIUS or TACACS+

Using RADIUS or TACACS+ over the local user database on the TransPort allows the use of a centralized server for user creation and control. If presented with the option to use either of these user management options, TACACS+ is viewed as the more secure of the two, and provides greater control over what the users are able and not able to do once in the systems it controls the users for.

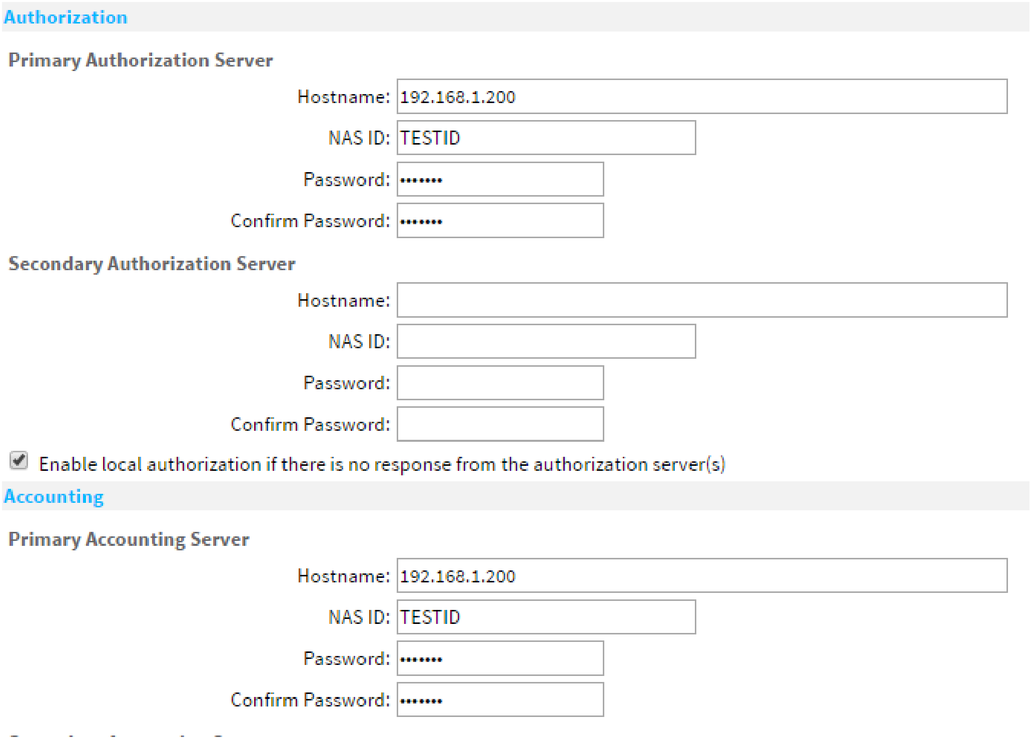
11.2 Enabling RADIUS

This section will cover configuring RADIUS settings on the TransPort. It will not cover setting up and installing the actual RADIUS server. See the user manuals of the desired RADIUS server for assistance in configuring the server.

11.2.1 WebUI Method

Navigate to **Configuration – Security > RADIUS > RADIUS Client0**.

If using both Authorization and Accounting, fill in the Hostname or IP of the RADIUS server, NAS ID, and password for the user, as shown below:



Authorization

Primary Authorization Server

Hostname: 192.168.1.200
NAS ID: TESTID
Password: •••••••
Confirm Password: •••••••

Secondary Authorization Server

Hostname:
NAS ID:
Password:
Confirm Password:

☑ Enable local authorization if there is no response from the authorization server(s)

Accounting

Primary Accounting Server

Hostname: 192.168.1.200
NAS ID: TESTID
Password: •••••••
Confirm Password: •••••••

NOTE: It is optional to enable the feature "**Enable local authorization if there is no response from the authorized server(s)**", for local user fall back if the RADIUS server is unreachable.

Ensure to **Apply** and **Save** the changes after they are made.

11.2.2 CLI Method

To enable RADIUS from the CLI, log into the TransPort using SSH, and issue the following commands:

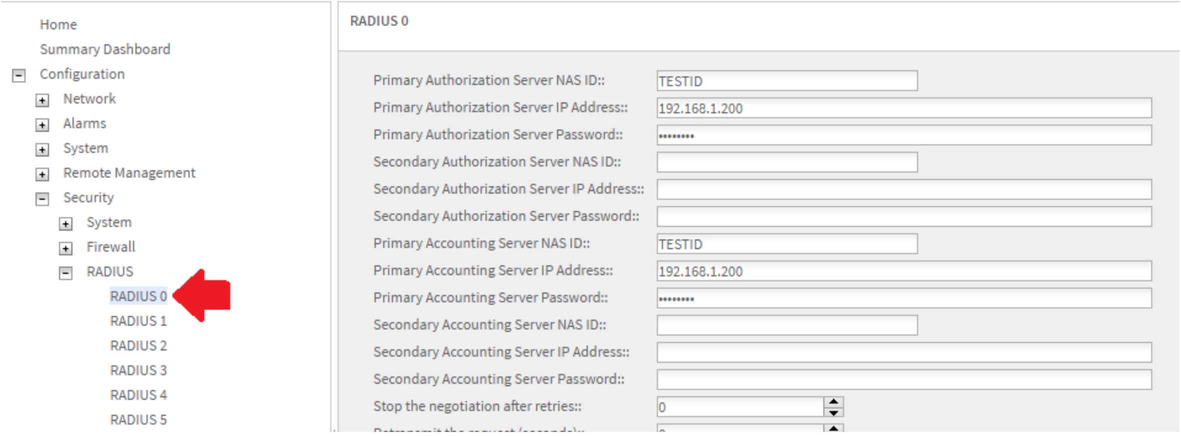
```
radcli 0 server 192.168.1.200       <- This sets the Authorization Server IP
radcli 0 nasid TESTID  <-  This sets the Authorization Server NAS ID
radcli 0 password password_to_set  <-  This sets the Authorization Server Password
radcli 0 aserver 192.168.1.200  <-  This sets the Accounting Server IP
radcli 0 anasid TESTID  <-  This sets the Accounting Server NAD ID
radcli 0 apassword password_to_set  <-  This sets the Accounting Server Password
config 0 save
```

This will enable RADIUS on the TransPort for Accounting and Authorization.

11.2.3 Digi Remote Manager Method

Within Digi Remote Manager, navigate to **Device Management > Devices**, and open up the **Properties** of the device to change.

Once on the Properties page, navigate to **Configuration > Security > RADIUS > RADIUS 0**. On this page, make the changes as shown below to add both the Authorization and Accounting server information:



RADIUS 0

Primary Authorization Server NAS ID:: TESTID
Primary Authorization Server IP Address:: 192.168.1.200
Primary Authorization Server Password:: ••••••••
Secondary Authorization Server NAS ID::
Secondary Authorization Server IP Address::
Secondary Authorization Server Password::
Primary Accounting Server NAS ID:: TESTID
Primary Accounting Server IP Address:: 192.168.1.200
Primary Accounting Server Password:: ••••••••
Secondary Accounting Server NAS ID::
Secondary Accounting Server IP Address::
Secondary Accounting Server Password::
Stop the negotiation after retries:: 0

Ensure to **Save** the changes after they are made.

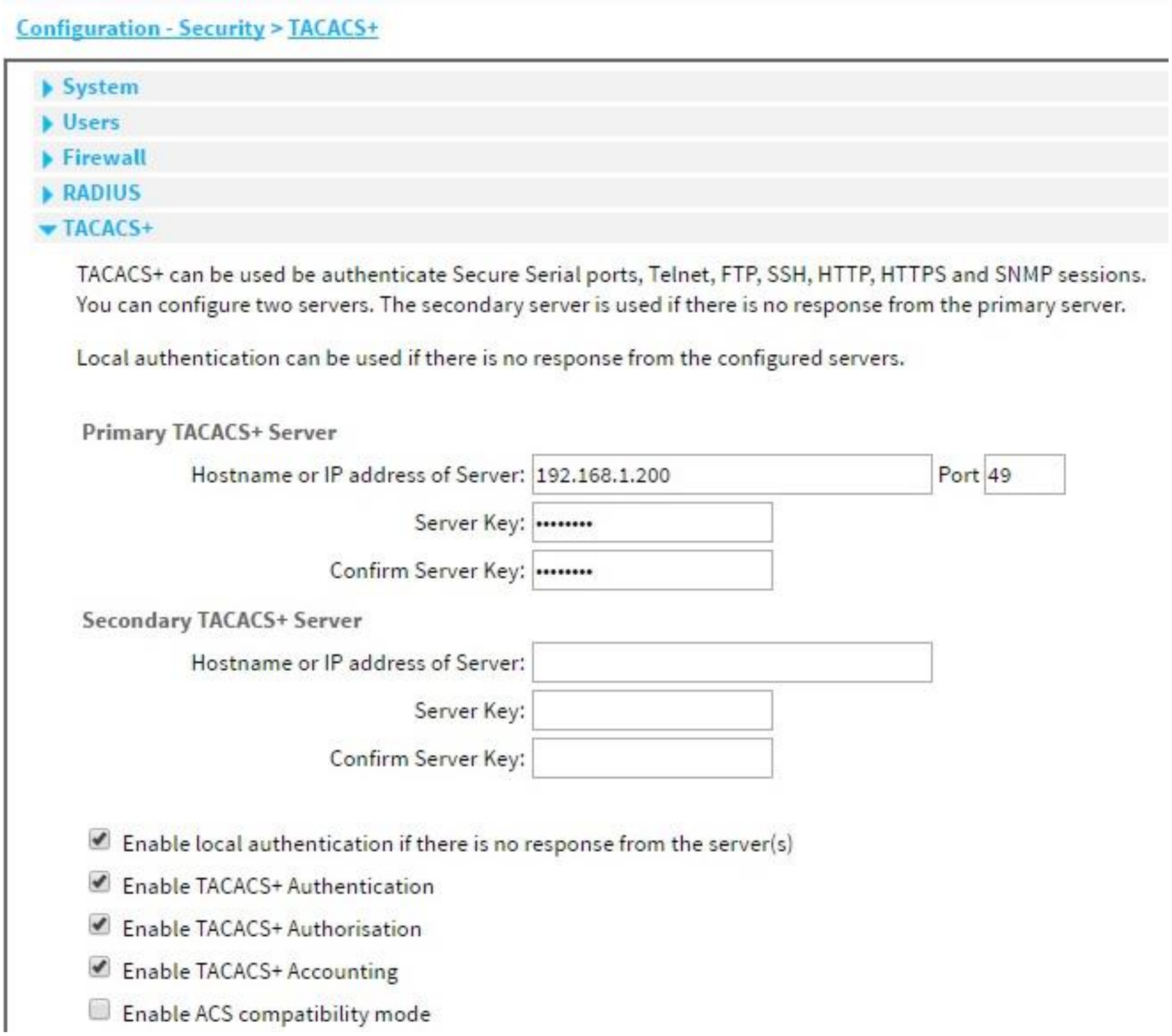
11.3 Enabling TACACS+

This section will cover configuring TACACS+ settings on the TransPort. It will not cover setting up and installing the actual TACACS+ server. See the user manuals of the desired TACACS+ server for assistance in configuring the server.

11.3.1 WebUI Method

Navigate to **Configuration – Security > TACACS+**.

Fill in the IP address, Port number (optional), and Server Key information for the TACACS+ Server. Also choose up to all 3 options for Authentication, Authorization, and Accounting, as shown on the next page:



TACACS+ can be used be authenticate Secure Serial ports, Telnet, FTP, SSH, HTTP, HTTPS and SNMP sessions. You can configure two servers. The secondary server is used if there is no response from the primary server.

Local authentication can be used if there is no response from the configured servers.

Primary TACACS+ Server

Hostname or IP address of Server: 192.168.1.200 Port 49

Server Key: ••••••••

Confirm Server Key: ••••••••

Secondary TACACS+ Server

Hostname or IP address of Server:

Server Key:

Confirm Server Key:

☑ Enable local authentication if there is no response from the server(s)

☑ Enable TACACS+ Authentication

☑ Enable TACACS+ Authorisation

☑ Enable TACACS+ Accounting

☐ Enable ACS compatibility mode

NOTE: It is optional to enable the feature "**Enable local authorization if there is no response from the authorized server(s)**", for local user fall back if the TACACS+ server is unreachable.

Click **Apply** to apply the settings. Once the settings are applied to the TransPort, access to the router under the current user will likely be lost as the device is now using TACACS+. **Log back in** to the router with a TACACS+ authorized user, and **Save** the changes that were just made.

11.3.2 CLI Method

To enable TACACS+ from the CLI, log into the TransPort using SSH, and issue the following commands:

tacplus 0 svr 192.168.1.200 <- This sets the TACACS+ Server IP
tacplus 0 authent on <- This enables Authentication for TACACS+
tacplus 0 author on <- This enables Authorization for TACACS+
tacplus 0 acct on <- This enables Accounting for TACACS+

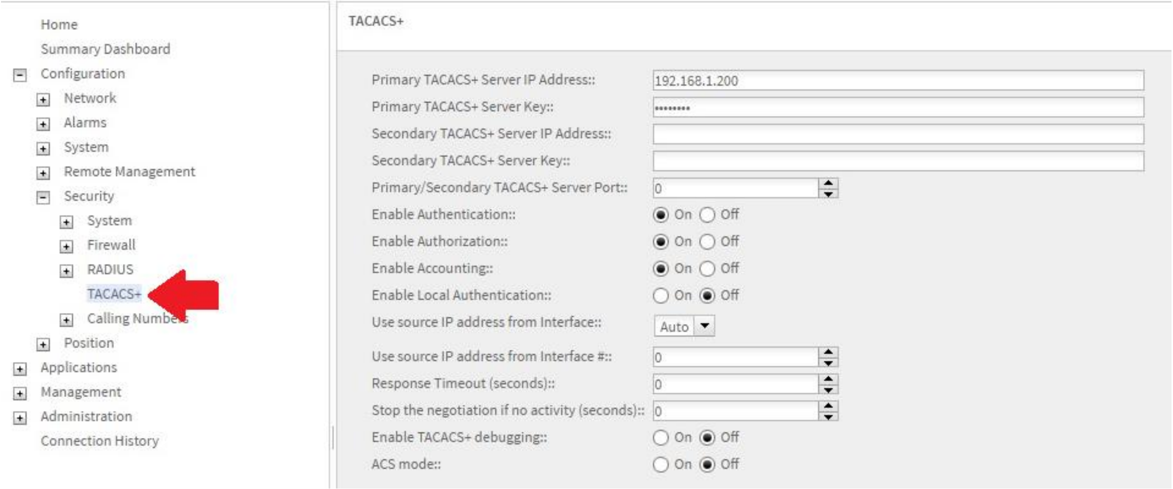
tacplus 0 localauth on <- This enables the local user authorization if TACACS+ is unreachable
config 0 save

This will enable TACACS+ on the TransPort for Authentication, Authorization, and Accounting.

11.3.3 Digi Remote Manager Method

Within Digi Remote Manager, navigate to **Device Management > Devices**, and open up the **Properties** of the device to change.

Once on the Properties page, navigate to **Configuration > Security > TACACS+**. On this page, make the changes as shown below to add the Server IP and Key, and Authentication, Authorization, and Accounting for TACACS+ usage:



TACACS+

Primary TACACS+ Server IP Address:: 192.168.1.200
Primary TACACS+ Server Key:: ••••••••
Secondary TACACS+ Server IP Address::
Secondary TACACS+ Server Key::
Primary/Secondary TACACS+ Server Port:: 0
Enable Authentication:: ● On ○ Off
Enable Authorization:: ● On ○ Off
Enable Accounting:: ● On ○ Off
Enable Local Authentication:: ○ On ● Off
Use source IP address from Interface:: Auto
Use source IP address from Interface #:: 0
Response Timeout (seconds):: 0
Stop the negotiation if no activity (seconds):: 0
Enable TACACS+ debugging:: ○ On ● Off
ACS mode:: ○ On ● Off

Ensure to **Save** the changes after they are made.

12 PHYSICAL SECURITY

12.1 Why Physical Security Important

Physical security of the TransPort is just as important as securing the device from digital attacks. Without the device being in a physically secure location, the equipment could potentially be damaged, or worse, stolen from the location they are installed in.

12.2 Security Recommendations

Below is a list of recommendations to consider when installing the TransPort routers:

1) Install the TransPort in a location secured with a lock and key, and limit personnel access to the location.
2) Disable unused ports on the TransPort using methods discussed previously in this guide.
3) Block unused interfaces with the firewall.
4) Disable the reset button.
5) Implement customer specific factory default configuration files if the device is returned to defaults for any reason.